UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,285	10/10/2000	John M. Hammer	05456.105008	4449

69151 7590 07/24/2009

KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA, GA 30309-3521

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
07/24/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JOHN M. HAMMER, RIXIN GE, CHARLES D. BURKE, and CHARLES HUBBARD

Appeal 2008-006295
Application 09/685,285[1]
Technology Center 2100

Decided: July 24, 2009[2]

Before LEE E. BARRETT, LANCE LEONARD BARRY and JAY P. LUCAS, *Administrative Patent Judges.*

LUCAS, *Administrative Patent Judge.*

DECISION ON APPEAL

---

[1] Application filed October 10, 2000. Application is a continuation-in-part of 09/663886, now abandoned. The real party in interest is IBM Internet Security Systems.

[2] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the Decided Date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

STATEMENT OF THE CASE

Appellants appeal from a final rejection of claims 1 to 9 and 11 to 65 under authority of 35 U.S.C. § 134(a). Claim 10 is cancelled. The Board of Patent Appeals and Interferences has jurisdiction under 35 U.S.C. § 6(b).

Appellants' invention relates to method for creating a record concerning security incidents and responses to them in a computer system. In the words of the Appellants:

> A security management system can log, investigate, respond, and track computer security incidents that can occur in a networked computer system. In other words, the security management system can produce a security record of information related to the tracking of suspicious computer activity or actual computer security threats, such as denial of service attacks or other similar compromises to computers or computer networks. The security record can include, but is not limited to, date and times of computer security incidents, a name for a particular security incident, a security management system user, and a potential source of the computer security incident. The security record can be designed as a running log that saves or records all activity of a computer incident source as well as the activity of the security team responding to the computer incident source. To produce the security record, all data that relates to a computer incident and all data that relates to a computer incident response can be sent to a separate protected database, where data is protected by digital signature algorithms (DSAs).

Spec 63.

Claim 1 is exemplary:

> 1. A method for automatically creating a record for one or more computer security incidents and reactions thereto, comprising the steps of:

recording computer security incident information with at least one of a date and time stamp, the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat;

classifying the computer security incident information;

automatically suggesting one or more computer security threat procedures based on a classification of the computer security incident information;

displaying the one or more suggested computer security threat procedures, each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information;

receiving a selection of a suggested computer security threat procedure from a user, the selection comprising one or more steps of the selected computer security threat procedure;

executing the selected one or more steps of the computer security threat procedure;

in response to executing the one or more steps of the selected computer security threat procedure, recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure with at least one of a date
and time stamp; and

outputting a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, an identity of the user who selected the computer security threat procedure, and at least one of a corresponding date stamp and time stamp.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Reps	US 6.070,190	May 30, 2000
Shostack	US 6,298,445	Oct. 2, 2001 (filed April 30, 1998)
Trcka	US 6,453,345	Sep. 17, 2002 (filed May 7, 1997)

REJECTIONS

The Examiner rejects the claims as follows:

R1: Claims 1 to 9, 11 to 50 and 56 to 65 stand rejected under 35 U.S.C. 103(a) for being obvious over Shostack in view of Trcka.

R2: Claims 51 to 55 stand rejected under 35 U.S.C. 103(a) for being obvious over Shostack in view of Reps.

The claims will be addressed in the order of the Appellants' arguments. Unless otherwise noted, claim 1 is representative. See 37 CFR § 1.41.37(c)(vii). *See also In re McDaniel*, 293 F.3d 1379, 1383 (Fed. Cir. 2002).

Appellants contend that the claimed subject matter is not rendered obvious by Shostack in combination with Trcka and Reps, for failure of the references singly and in combination to teach or suggest certain of the claimed limitations. The Examiner contends that each of the claims is properly rejected.

Rather than repeat the arguments of Appellants or the Examiner, we make reference to the Briefs and the Answer for their respective details. Only those arguments actually made by Appellants have been considered in this opinion. Arguments which Appellants could have made but chose not to make in the Briefs have not been considered and are deemed to be waived.

We affirm the rejections.

ISSUE

The issue is whether Appellants have shown that the Examiner erred in rejecting the claims under 35 U.S.C. § 103(a). The issue turns on whether Shostack, supported by Trcka or Reps, teach the display of suggested procedures to follow when faced with a security threat and allow the selection of one of the procedures, and other limitations as claimed.

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence.

1. Appellants have invented a security system management method which helps a user investigate and respond to security incidents that may occur in a large computer system. (Spec 4, l. 23). The system suggests to the user possible responses to the incident, and produces a log record of the event, the actual procedures that were carried out, the category of the incident, the date and time and other related attributes concerning the event. (Spec 5, l. 8 to l. 31).

2. The Shostack patent addresses monitoring and security needs of a network administrator by offering a system to provide information and updates in response to security breaches, both potential and happening. (col. 2, ll. 48-60). On detection of an intrusion, the breach is detected, investigated and located. (col. 6, ll. 53 – 60). A user is given a choice of solutions. (col. 2, l. 49). The system provides a report of all the breaches, including the solution and other relevant information. (col. 7, l. 24). The breaches are logged and reported. (col. 13, l. 42).

3. The Trcka patent presents a Network Security and Surveillance System for monitoring and analyzing traffic on a network, including reporting on viruses and break-ins. (col. 2, l. 61). The logs show the date and times of the occurrences of the incidents. (Fig. 19, col. 15, l. 64). The user is given choices on the reactions to events, including setting alarms. (col. 17, l. 31).

4. The Reps patent teaches a monitoring and alerting system for a network. (col. 1, l. 25 to 50). Graphs and tables report on elements on the network, such as servers, indicating performance and operations data in tabular form. (col. 4, l. 53; Fig. 9).

PRINCIPLES OF LAW

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. See *In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of prima facie obviousness or by rebutting the prima facie case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)).

"In reviewing the [E]xaminer's decision on appeal, the Board must necessarily weigh all of the evidence and argument." *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

When "non functional descriptive material" is recorded or stored in a memory or other medium (i.e., substrate) it is treated as analogous to printed matter cases where what is printed on a substrate bears no functional

relationship to the substrate and is given no patentable weight. *See In re Gulack,* 703 F.2d 1381, 1385 (Fed. Cir. 1983) ("Where the printed matter is not functionally related to the substrate, the printed matter will not distinguish the invention from the prior art in terms of patentability. Although the printed matter must be considered, in that situation it may not be entitled to patentable weight."). *See also Ex parte Curry,* 84 USPQ2d 1272 (BPAI 2005) (nonprecedential) (Federal Circuit Appeal No. 2006-1003, *aff'd* Rule 36 Jun. 12, 2006). The Examiner need not give patentable weight to descriptive material absent a new and unobvious functional relationship between the descriptive material and the substrate. *See In re Lowry,* 32 F.3d 1579, 1582-83 (Fed. Cir. 1994); *In re Ngai*, 367 F.3d 1336, 1338 (Fed. Cir. 2004).

ANALYSIS

From our review of the administrative record, we find that Examiner has rejected all of Appellants' claims under 35 U.S.C. § 103(a). The Examiner's case is presented on pages 3 to 26 of the Examiner's Answer[3]. In opposition, Appellants present a number arguments.

Arguments with respect to the rejection of claims 1 to 9, 11 to 50 and 56 to 65 under 35 U.S.C. § 103(a) [R1]

Appellants first contend that Shostack does not teach or suggest displaying "one or more procedures comprising one or more steps or provide for the reception of a selection of one or more procedures comprising one or

[3] We observe that claims 1 to 9 and 11 to 65 include the term "automatically" in the preamble and body of the independent claims, so we are interpreting them to rely upon a machine for performance of the claimed methods, as opposed to being comprised of manually performed steps.

more steps." (Brief 15, middle). We do not find this contention supported by the references. First, Shostack teaches that the user is provided with at least one choice, namely requesting an enhancement to deal with a security attack, or authorizing the system to do that automatically. (Col. 2, l. 50). In addition, we find that the Examiner has relied upon the secondary reference Trcka to supply the teaching of "provide for the reception of a selection of one or more procedures comprising one or more steps," as described in the Answer. (Answer 28, top). We do not find error in the application of the art as indicated by the Examiner.

Appellants further contend that Shostack does not provide a teaching of storage of the type of log information required by the claims. (Brief 15, bottom). The Examiner Answer itemizes the types of information taught stored by the Shostack patent. (Answer, p. 30-31). We agree that the requirements of the claims are satisfied by this reference.

Appellants argue that Trcka does not teach the claimed date and time stamp on the output record of an incident. The claim requires only one of time or date, but the Trcka reference shows both. (See FF3 above.)

With regard to claim 42, Appellants contend that neither Shostack nor Trcka teach or disclose the displaying procedures or receiving the user's selection steps of that claim. They also contend that the storing step is not satisfied. We have reviewed the Examiner lengthy exposition of the teachings in Shostack and Trcka (Answer, p. 33-35) and are convinced that the rejection was not in error for the reasons stated by the Examiner.

Appellants arguments with regard to claim 56 (Brief 22) are similar to those discussed above concerning claim 1, and are not convincing for the reasons stated.

Arguments with respect to the rejection of claims 51 to 55 under 35 U.S.C. § 103(a) [R2]

The Examiner has rejected claims 51 to 55 for being obvious over Shostack in view of Reps. This is labeled as a new rejection only because the order of the references has been reversed. We note the Appellants indicated in the Reply that the Brief is still valid as it was prepared "irrespective of the order of the presentation of the references." (Reply 4, middle).

Appellants argue that Reps and Shostack do not teach accessing a table comprising computer locations, Internet address ranges and other related information. (Brief 20, middle). As this information is not utilized in the claims to perform a function, we find the exact nature of what is written to the storage device is a non-functional limitation that need not be given weight. (See *In re Gulack* cited above.) Nonetheless, the Examiner has listed in detail the citations in Shostack and Reps on which the specific limitation were found (Answer 36 to 38, 34) and has established a sufficient record to support the rejection under 35 U.S.C. § 103 obviousness.

Finally, Appellants argue that the references do not teach storing a permanent record as claimed in claim 51. (Brief 21, middle). The issue of the storage has been addressed above with regard to claim 1, and the arguments were not found convincing.

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude that the Examiner did not err in rejecting claims 1 to 9 and 11 to 65 under 35 U.S.C. § 103(a) [R1 and R2].

DECISION

R1: The rejection of claims 1 to 9, 11 to 50 and 56 to 65 under 35 U.S.C. 103(a) for being obvious over Shostack in view of Trcka is affirmed.

R2: The rejection of claims 51 to 55 under 35 U.S.C. 103(a) for being obvious over Shostack in view of Reps is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

PEB

KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA GA 30309-3521